The Value 4 of Binary Kloosterman Sums

Jean-Pierre Flori, Sihem Mesnager, Gérard Cohen

The Value 4 of Binary Kloosterman Sums

Jean-Pierre Flori * Sihem Mesnager † Gérard Cohen *

Tuesday 5th July, 2011

Abstract

Kloosterman sums have recently become the focus of much research, most notably due to their applications in cryptography and their relations to coding theory.

Very recently Mesnager has showed that the value 4 of binary Kloosterman sums gives rise to several infinite classes of bent functions, hyper-bent functions and semi-bent functions in even dimension.

In this paper we analyze the different strategies used to find zeros of binary Kloosterman sums to develop and implement an algorithm to find the value 4 of such sums. We then present experimental results showing that the value 4 of binary Kloosterman sums gives rise to bent functions for small dimensions, a case with no mathematical solution so far.

1 Introduction

Kloosterman sums have recently become the focus of much research and are actively studied for their applications in cryptography, coding theory, and other fields. We denote by $K_m(a)$, for $a \in \mathbb{F}_{2^m}$, the so-called classical binary Kloosterman sum over $\mathbb{F}_{2^m}$. Lachaud and Wolfmann have proved in [22] that $K_m(a)$ takes all values multiple of 4 in the range $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$.

It has been proved that both the values 0 and 4 of $K_m(a)$ lead to construct several special important classes of Boolean functions [6] such as bent functions (introduced by Rothaus [31] in 1972), hyper-bent functions (introduced by Youssey and Gong [41] in 2002) and semi-bent functions (introduced by Chee, Lee and Kim [9] in 1994) in even dimension. All such functions are used in various areas and are of great interest in the fields of cryptography and communication, since they play a prominent role in the security of cryptosystems. For example they play an important role in the design of hash functions and of stream and block ciphers.

It is known since 1974 that the zeros of $K_m(a)$ give rise to bent functions, but it is only in 2009 that Mesnager [28] has proved that the value 4 for $K_m(a)$ also leads to construction of bent and hyper-bent functions. Some authors have proposed algorithms for testing the zeros of binary Kloosterman sums, but until now no algorithm has been proposed in the literature to test or find the value 4 of binary Kloosterman sums. In this paper we are interested precisely in studying the various algorithms to test whether $K_m(a) = 4$ or not for a given $a \in \mathbb{F}_{2^m}$ or to find an a giving value 4.

The paper is organized as follows. In Sect. 2 we give some background on Boolean functions, binary Kloosterman sums and elliptic curves over finite fields. In Sect. 3 we recall classical results

*Institut Télécom, Télécom ParisTech, UMR 7539, CNRS LTCI, 46 rue Barrault, F-75634 Paris Cedex 13, France {flori,cohen}@enst.fr

†LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, Department of Mathematics, University of Paris XIII and University of Paris VIII, 2 rue de la liberté, 93526 Saint-Denis Cedex, France smesnager@univ-paris8.fr

about divisibility of binary Kloosterman sums and give alternate proofs of such results involving the theory of elliptic curves. In Sect. 4 we first present different algorithms to test and find specific values of binary Kloosterman sums. Then, emphasizing the specificity of the zero case, we study the use of elliptic curves involved in this case, explain which results can be extended to the value 4, develop and implement an algorithm to find that value. In Sect. 5 we present experimental results showing that all the values 4 of binary Kloosterman sums for $4 \leq m \leq 16$, m even, give rise to bent functions, what was not known before.

2 Notation and Preliminaries

For any set S, S^* denotes $S^* = S \setminus \{0\}$ and $\#S$ the cardinality of S. Unless stated otherwise, m will be a positive integer greater than 3 and a an element of $\mathbb{F}_{2^m}$ used to define (hyper, semi)-bent Boolean functions with $n = 2m$ inputs.

2.1 Background on Boolean Functions

A Boolean function f on $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function on the Galois field $\mathbb{F}_{2^n}$ of order 2^n. The *weight* of f, denoted by $\mathrm{wt}(f)$, is the *Hamming weight* of the image vector of f, i.e. the cardinality of its support $\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

For any positive integer k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$ will be denoted by $\mathrm{Tr}_r^k(\cdot)$. It can be defined as:

$$\mathrm{Tr}_r^k(x) = \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}} \quad .$$

In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Every non-zero Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion of the form:

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)}\left(a_j x^j\right) + \epsilon(1 + x^{2^n-1}), \quad a_j \in \mathbb{F}_{2^{o(j)}}$$

called its polynomial form, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$, the most usual choice being the smallest element in each cyclotomic class, called the coset leader of the class, $o(j)$ is the size of the cyclotomic coset containing j, and $\epsilon = \mathrm{wt}(f)$ modulo 2. Recall that, given an integer e, $0 \leq e \leq 2^n - 1$, with binary expansion: $e = \sum_{i=0}^{n-1} e_i 2^i$, $e_i \in \{0, 1\}$, the 2-weight of e, denoted by $w_2(e)$, is the Hamming weight of the binary vector $(e_0, e_1, \ldots, e_{n-1})$.

Let f be a Boolean function on $\mathbb{F}_{2^n}$. Its *"sign" function* is the integer-valued function $\chi(f) = \chi_f = (-1)^f$. The *Walsh-Hadamard transform* of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as:

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(\omega x)} \quad .$$

Bent functions are functions with maximum non-linearity. They only exist for even number of inputs and can be defined as follows.

Definition 1. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be bent if $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$, for all $\omega \in \mathbb{F}_{2^n}$.*

Hyper-bent functions have even stronger properties than bent functions. More precisely, hyper-bent functions can be defined as follows.

Definition 2. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be hyper-bent if the function $x \mapsto f(x^i)$ is bent, for every integer i co-prime with $2^n - 1$.*

Semi-bent functions exist for even or odd number of inputs. We will only be interested in even number of inputs where they can be defined as follows.

Definition 3. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+2}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$.*

2.2 Binary Kloosterman Sums and (Hyper, Semi)-Bentness Property

The classical binary Kloosterman sums on $\mathbb{F}_{2^m}$ are defined as follows.

Definition 4. *The binary Kloosterman sums on $\mathbb{F}_{2^m}$ are:*

$$K_m(a) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)}, \quad a \in \mathbb{F}_{2^m} \ .$$

Note that we assume $\mathrm{Tr}_1^m\left(\frac{1}{0}\right) = \mathrm{Tr}_1^m\left(0^{2^{m-1}-1}\right) = 0$. It is an elementary fact that $K_m(a) = K_m(a^2)$:

$$\begin{aligned} K_m(a) &= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m\left(ax + \frac{1}{x}\right)} = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m\left(a^2x^2 + \frac{1}{x^2}\right)} \\ &= \sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m\left(a^2x + \frac{1}{x}\right)} = K_m(a^2) \ . \end{aligned}$$

It has been shown that the zeros of binary Kloosterman sums lead to bent, hyper-bent and semi-bent functions. We summarize the known results in Table 1:

- A class of functions is given in terms of $a \in \mathbb{F}_{2^m}$; remember that $a \in \mathbb{F}_{2^m}$, but that the corresponding Boolean functions have $n = 2m$ inputs.
- Unless stated otherwise, the given conditions on a are necessary and sufficient for the Boolean functions to verify the given property.

Similarly the value 4 of binary Kloosterman sums gives rise to bent, hyper-bent and semi-bent functions. We summarize the known results about (hyper)-bent function in Table 2 and those about semi-bent functions in Table 3. The conventions are the same as for Table 1.

Hence it is of cryptographic interest to study divisibility properties of binary Kloosterman sums and develop efficient algorithms to find specific values of such sums or test their values.

2.3 Elliptic Curves over Finite Fields

In this subsection, we present some classical results about elliptic curves over finite fields, as well as their connections with binary Kloosterman sums.

Let m be a positive integer, $\mathbb{F}_q$ the finite field of characteristic p with $q = p^m$ and $\overline{\mathbb{F}_q}$ its algebraic closure. Let E be an elliptic curve defined over $\mathbb{F}_q$ and given by a Weierstrass equation [35, Chapter III]:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ .$$

Table 1: Families of (hyper)-bent and semi-bent functions for $K_m(a) = 0$

Class of functions	Property	Conditions	References
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$; $\gcd(r, 2^m+1) = 1$	hyper-bent	$K_m(a) = 0$	[13, 22, 24, 7]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$; $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $\gcd(r, 2^m+1) = 1$	semi-bent	$K_m(a) = 0$	[29]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{4}+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, $\gcd(r, 2^m+1) = 1$, m odd	semi-bent	$K_m(a) = 0$	[29]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{(2^m-1)3+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, $\gcd(r, 2^m+1) = 1$	semi-bent	$K_m(a) = 0$	[29]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{6}+1}\right)$; $\mathrm{Tr}_m^n(c) = 1$, $\gcd(r, 2^m+1) = 1$, m even	semi-bent	$K_m(a) = 0$	[29]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(\alpha x^{2^m+1}\right) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{\nu-1}-1} x^{(2^m-1)\frac{i}{2^\nu}+1}\right)$; $\gcd(r, 2^m+1) = 1$, $\gcd(\nu, m) = 1$, $\mathrm{Tr}_m^n(\alpha) = 1$,	semi-bent	$K_m(a) = 0$	[29]

Table 2: Families of (hyper)-bent functions for $K_m(a) = 4$

Class of functions	Property	Conditions	References
$\mathrm{Tr}_1^n\left(a\zeta^i x^{3(2^m-1)}\right) + \mathrm{Tr}_1^2\left(\beta^j x^{\frac{2^n-1}{3}}\right)$; m odd and $m \not\equiv 3 \pmod 6$, β is a primitive element of $\mathbb{F}_4$, ζ is a generator of the cyclic group U of (2^m+1)-th roots of unity, $(i,j) \in \{0,1,2\}^2$	hyper-bent	$K_m(a) = 4$ and $\mathrm{Tr}_1^m\left(a^{1/3}\right) = 0$	[27]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m odd, $\gcd(r, 2^m+1) = 1$	hyper-bent	$K_m(a) = 4$	[28]
$\mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m even	bent	$K_m(a) = 4$ (necessary condition)	[28]

Table 3: Families of semi-bent functions for $K_m(a) = 4$

Class of functions	Property	Conditions	References
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right)$; $b \in \mathbb{F}_4^*$ and $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $\gcd(r, 2^m+1) = 1$, m odd	semi-bent	$K_m(a) = 4$	[29]
$\mathrm{Tr}_1^n\left(ax^{3(2^m-1)}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; m odd and $m \not\equiv 3 \pmod 6$	semi-bent	$K_m(a) = 4$	[29]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{(2^m-1)\frac{1}{4}+1}\right)$; $b \in \mathbb{F}_4^*$, $\mathrm{Tr}_m^n(c) = 1$, $\gcd(r, 2^m+1) = 1$, m odd	semi-bent	$K_m(a) = 4$	[29]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) + \mathrm{Tr}_1^n\left(cx^{(2^m-1)\frac{1}{2}+1}\right) + \mathrm{Tr}_1^n\left(x^{3(2^m-1)+1}\right)$; $b \in \mathbb{F}_4^*$, $\mathrm{Tr}_m^n(c) = 1$, $\gcd(r, 2^m+1) = 1$, m odd	semi-bent	$K_m(a) = 4$	[29]
$\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right) + \mathrm{Tr}_1^n\left(\alpha x^{2^m+1}\right) + \mathrm{Tr}_1^n\left(\sum_{i=1}^{2^{\nu-1}-1} x^{(2^m-1)\frac{i}{2^\nu}+1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$; $b \in \mathbb{F}_4^*$; $\gcd(r, 2^m+1) = 1$, $\gcd(\nu, m) = 1$, $\mathrm{Tr}_m^n(\alpha) = 1$, m odd	semi-bent	$K_m(a) = 4$	[29]

We denote by O_E the point at infinity of E (i.e. the neutral point for the addition law), by $[n]$ the multiplication by an integer n on E and by $\mathrm{End}(E) = \mathrm{End}_{\overline{\mathbb{F}_q}}(E)$ the ring of endomorphisms of E over the algebraic closure $\overline{\mathbb{F}_q}$. Over $\overline{\mathbb{F}_q}$, elliptic curves are classified up to isomorphism by their j-invariant.

The group of rational points of E over an extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ (i.e. points with coordinates in $\mathbb{F}_q$) is denoted by $E(\mathbb{F}_{q^k})$; the number of points of this group by $\#E(\mathbb{F}_{q^k})$. When the context is clear, we denote $\#E(\mathbb{F}_q)$ simply by $\#E$. It is a classical result that $\#E = q + 1 - t$ where t is the trace of the Frobenius automorphism of E over $\mathbb{F}_q$ and the following theorem has been shown by Hasse.

Theorem 5 ([35, Theorem V.2.3.1])**.** *Let t be the trace of the Frobenius automorphism of an elliptic curve over $\mathbb{F}_q$, then:*

$$|t| \leq 2\sqrt{q} \ .$$

For an integer n, we denote by $E[n]$ the n-torsion subgroup of the points of E over $\overline{\mathbb{F}_q}$, i.e.

$$E[n] = \{P \in E(\overline{\mathbb{F}_q}) \mid [n]P = O_E\} \ .$$

The subgroup of rational points of n-torsion is denoted by $E[n](\mathbb{F}_q) = E[n] \cap E(\mathbb{F}_q)$. The following classical result gives the structure of the groups of torsion points.

Proposition 6 ([35, Corollary III.6.4])**.** *Let n be a positive integer.*

- *If $p \nmid n$, then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*
- *One of the following is true: $E[p^e] \simeq \{0\}$ for all $e \geq 1$ or $E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$ for all $e \geq 1$.*

It can also be shown that a point of E is of n-torsion if and only if its coordinates are roots of a bivariate polynomial called the n-division polynomial of E [3, Section III.4]. In fact one can even choose a univariate polynomial in the x coordinate that we denote by f_n.

Here we will be interested in *ordinary* elliptic curves which can be defined as follows.

Definition 7 ([35, Theorem V.3.1])**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$ and t the trace of the Frobenius automorphism of E. We say that E is ordinary if it verifies one of the following equivalent properties:*

- *$p \nmid t$;*
- *$E[p] \simeq \mathbb{Z}/p\mathbb{Z}$;*
- *$\mathrm{End}(E)$ is an order in an imaginary quadratic extension of $\mathbb{Q}$.*

If E is not ordinary, we say it is *supersingular*.

Finally, using classical results of Deuring [12] and Waterhouse [39], the number of ordinary elliptic curves (up to isomorphism) with a given trace t of the Frobenius automorphism (or equivalently a number of points $q + 1 - t$), verifying $|t| \leq 2\sqrt{q}$ and $p \nmid t$, can be computed as follows. This property indeed implies that $\mathrm{End}(E)$ must be an order $\mathcal{O}$ in $K = \mathbb{Q}[\alpha]$ and contains the order $\mathbb{Z}[\alpha]$ of discriminant Δ where $\alpha = \frac{t+\sqrt{\Delta}}{2}$ and $\Delta = t^2 - 4q$. We denote by $H(\Delta)$ the *Kronecker class number* [33, 11]:

$$H(\Delta) = \sum_{\mathbb{Z}[\alpha] \subset \mathcal{O} \subset K} h(\mathcal{O}) \ ,$$

where the sum is taken over all the orders $\mathcal{O}$ in K containing $\mathbb{Z}[\alpha]$ and $h(\mathcal{O})$ is the classical class number.

Proposition 8 ([33, 19, 11]). *Let t be an integer such that $|t| \leq 2\sqrt{q}$ and $p \nmid t$. The number $N(t)$ of elliptic curves over $\mathbb{F}_q$ with $q+1-t$ rational points is given by:*

$$N(t) = H(\Delta) \ ,$$

where $\Delta = t^2 - 4q$.

It should be noted that $H(\Delta)$ can be computed from the value of the classical class number of (the maximal order of) K using the following proposition.

Proposition 9 ([23, 11, 19, 10]). *Let $\mathcal{O}$ be the order of conductor f in K, an imaginary quadratic extension of $\mathbb{Q}$, , $\mathcal{O}_K$ the maximal order of K and Δ_K the discriminant of (the maximal order of) K. Then:*

$$h(\mathcal{O}) = \frac{f h(\mathcal{O}_K)}{[\mathcal{O}_K^* : \mathcal{O}^*]} \prod_{p|f} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \ ,$$

where $\left(\frac{\cdot}{p}\right)$ is the Kronecker symbol.

Denoting the conductor of $\mathbb{Z}[\alpha]$ by f, $H(\Delta)$ can then be written as:

$$H(\Delta) = h(\mathcal{O}_K) \sum_{d|f} \frac{d}{[\mathcal{O}_K^* : \mathcal{O}]} \prod_{p|d} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \ .$$

We now give results specific to characteristic 2. First, E is supersingular if and only if its j-invariant is 0. Second, if E is ordinary, then its Weierstrass equation can be chosen to be of the form:

$$E : y^2 + xy = x^3 + bx^2 + a \ ,$$

where $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, its j-invariant is then $1/a$; moreover its first division polynomials are given by [20, 3]:

$$f_1(x) = 1, \quad f_2(x) = x, \quad f_3(x) = x^4 + x^3 + a, \quad f_4(x) = x^6 + ax^2 \ .$$

The quadratic twist of E is an elliptic curve with the same j-invariant as E, so isomorphic over the algebraic closure $\overline{\mathbb{F}_q}$, but not over $\mathbb{F}_q$ (in fact it becomes so over $\mathbb{F}_{q^2}$). It is unique up to isomorphism and we denote it by $\widetilde{E}$. It is given by the Weierstrass equation:

$$\widetilde{E} : y^2 + xy = x^3 + \widetilde{b}x^2 + a \ ,$$

where $\widetilde{b}$ is any element of $\mathbb{F}_q$ such that $\mathrm{Tr}_1^m\left(\widetilde{b}\right) = 1 - \mathrm{Tr}_1^m(b)$ [15]. The trace of its Frobenius automorphism is given by the opposite of the trace of the Frobenius automorphism of E, so that their number of rational points are closely related [15, 3]:

$$\#E + \#\widetilde{E} = 2q + 2 \ .$$

Lachaud and Wolfmann [21] (see also [19]) proved the following well-known theorem which gives a connection between binary Kloosterman sums and elliptic curves.

Theorem 10 ([21, 19]). *Let $m \geq 3$ be any positive integer, $a \in \mathbb{F}_{2^m}^*$ and $E_m(a)$ the elliptic curve defined over $\mathbb{F}_{2^m}$ by the equation:*

$$E_m(a) : y^2 + xy = x^3 + a \ .$$

Then:

$$\#E_m(a) = 2^m + K_m(a) \ .$$

3 Divisibility of Binary Kloosterman Sums

3.1 Classical Results

Because of their cryptographic interest, divisibility properties of Kloosterman sums have been studied in several recent papers. The following proposition is directly obtained from the result of Lachaud and Wolfmann [22].

Proposition 11 ([22]). *Let $m \geq 3$ be a positive integer. The set $\{K_m(a), a \in \mathbb{F}_{2^m}\}$ is the set of all the integers multiple of 4 in the range $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$.*

This result states in particular that binary Kloosterman sums are always divisible by 4. Afterwards several papers studied divisibility properties of binary Kloosterman sums by multiples of 4 and other integers.

The following classical result was first proved by Helleseth and Zinoviev [18] and classifies the values of $K_m(a)$ modulo 8 according to the value of the absolute trace of a.

Proposition 12 ([18]). *Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}$. Then $K_m(a) \equiv 0 \pmod 8$ if and only if $\mathrm{Tr}_1^m(a) = 0$.*

In the same article, they gave the following sufficient conditions to get certain values of $K_m(a)$ modulo 3.

Proposition 13 ([18]). *Let $m \geq 3$ be any positive integer and $a \in \mathbb{F}_{2^m}^*$. Suppose that there exists $t \in \mathbb{F}_{2^m}^*$ such that $a = t^4 + t^3$.*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$.*
- *If m is even, then $K_m(a) \equiv 0 \pmod 3$ if $\mathrm{Tr}_1^m(t) = 0$ and $K_m(a) \equiv -1 \pmod 3$ if $\mathrm{Tr}_1^m(t) = 1$.*

Furthermore Charpin, Helleseth and Zinoviev gave in [8] additional results about values of $K_m(a)$ modulo 3.

Proposition 14 ([8]). *Let $a \in \mathbb{F}_{2^m}^*$. Then we have:*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$ if and only if $\mathrm{Tr}_1^m\left(a^{1/3}\right) = 0$. This is equivalent to $a = \frac{b}{(1+b)^4}$ for some $b \in \mathbb{F}_{2^m}^*$.*
- *If m is even, then $K_m(a) \equiv 1 \pmod 3$ if and only if $a = b^3$ for some b such that $\mathrm{Tr}_2^m(b) \neq 0$.*

Most of these results about divisibility were first proved studying the link between exponential sums and coset weight distribution [18, 8]. However some of them can be proved in a completely different manner as we show in the next subsection.

3.2 Using Torsion of Elliptic Curves

Theorem 10 giving the value of $K_m(a)$ as the cardinality of an elliptic curve can indeed be used to deduce divisibility properties of binary Kloosterman sums from the rich theory of elliptic curves. We recall that the quadratic twist of $E_m(a)$ that we denote by $\widetilde{E}_m(a)$ is given by:

$$\widetilde{E}_m(a) : y^2 + xy = x^3 + bx^2 + a \ ,$$

where $b \in \mathbb{F}_{2^m}$ has absolute trace 1; it has cardinality:

$$\#\widetilde{E}_m(a) = 2^m + 2 - K_m(a) \ .$$

First of all, we recall a proof of the divisibility by 4 stated in Proposition 11 which is already mentioned in [1]. For $m \geq 3$, $K_m(a) \equiv \#E_m(a) \pmod 4$, so $K_m(a) \equiv 0 \pmod 4$ if and only if $\#E_m(a) \equiv 0 \pmod 4$. This is equivalent to $E_m(a)$ having a non-trivial rational point of 4-torsion. This can also be formulated as both the equation of $E_m(a)$ and its 4-division polynomial $f_4(x) = x^6 + ax^2$ having a rational solution. It is easily seen that $P = (a^{1/4}, a^{1/2})$ is always a non-trivial solution to this problem.

Then Lisoněk gave in [26] a similar proof of Proposition 12. Indeed, for $m \geq 3$, $K_m(a)$ is divisible by 8 if and only if $E_m(a)$ has a non-trivial rational point of 8-torsion. This is easily shown to be equivalent to $\mathrm{Tr}_1^m\left(a^{1/4}\right) = \mathrm{Tr}_1^m(a) = 0$.

Finally it is possible to prove directly that the condition given in Proposition 13 is not only sufficient, but also necessary, using torsion of elliptic curves. We use this property in Subsection 4.3.

Proposition 15. *Let $a \in \mathbb{F}_{2^m}^*$.*

- *If m is odd, then $K_m(a) \equiv 1 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.*
- *If m is even, then:*
  - *$K_m(a) \equiv 0 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 0$;*
  - *$K_m(a) \equiv -1 \pmod 3$ if and only if there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$ and $\mathrm{Tr}_1^m(t) = 1$.*

Proof. According to Proposition 13 we only have to show that if a verifies the given congruence, it can be written as $a = t^4 + t^3$.

- We begin with the case m odd, so that $2^m \equiv -1 \pmod 3$. Then $K_m(a) \equiv 1 \pmod 3$ if and only if $\#E_m(a) \equiv 0 \pmod 3$, i.e. if $E_m(a)$ has a non-trivial rational point of 3-torsion. It implies that the 3-division polynomial of $E_m(a)$ given by $f_3(x) = x^4 + x^3 + a$ has a rational solution, so that there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.
- Suppose now that m is even, so that $2^m \equiv 1 \pmod 3$.
  - If $K_m(a) \equiv -1 \pmod 3$, then $\#E_m(a) \equiv 0 \pmod 3$, and as in the previous case we can find $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.
  - If $K_m(a) \equiv 0 \pmod 3$, then $\#E_m(a) \equiv 1 \pmod 3$, but $\#\widetilde{E}_m(a) \equiv 0 \pmod 3$. The 3-division polynomial of $\widetilde{E}_m(a)$ is also given by $f_3(x) = x^4 + x^3 + a$, so that there exists $t \in \mathbb{F}_{2^m}$ such that $a = t^4 + t^3$.

□

4 Finding Specific Values of Binary Kloosterman Sums

4.1 Generic Strategy

In this section we present the most generic method to find specific values of binary Kloosterman sums. To this end one picks random elements of $\mathbb{F}_{2^m}$ and computes the corresponding values

until a correct one is found. Before doing any complicated computations, divisibility conditions as those stated in the previous section can be used to restrict the pool of elements to those satisfying certain conditions (but without missing any of them) or to filter out elements which will give inadequate values.

Then the most naïve method to check the value of a binary Kloosterman sum is to compute it as a sum. However one test would need $O(2^m m \log^2 m \log\log m)$ bit operations and this is evidently highly inefficient. Theorem 10 tells that this costly computation can be replaced by the computation of the cardinality of an elliptic curve over a finite field of characteristic 2. Using p-adic methods *à la Satoh* [32], also known as canonical lift methods, this can be done quite efficiently in $O(m^2 \log^2 m \log\log m)$ bit operations and $O(m^2)$ memory [17, 38, 37, 25]. Working with elliptic curves also has the advantage that one can check that the current curve is a good candidate before computing its cardinality as follows: one picks a random point on the curve and multiply it by the targeted order; if it does not give the identity on the curve, the curve does not have the targeted cardinality.

Finally it should be noted that, if ones looks for all the elements giving a specific value, a different strategy can be adopted as noted in [1]. Indeed a binary Kloosterman sum can be seen as Walsh-Hadamard transform of the Boolean function $\mathrm{Tr}_1^m(1/x)$. Therefore we can construct the Boolean function corresponding to the function $\mathrm{Tr}_1^m(1/x)$ and then use a fast Walsh-Hadamard transform to compute the value of all binary Kloosterman sums. Building the Boolean function costs one multiplication per element, so $O(2^m m \log m \log\log m)$ bit operations and $O(2^m)$ memory. The complexity of the fast Walsh-Hadamard transform is $O(2^m m^2)$ bit operations and $O(2^m m)$ memory [2].

4.2 Zeros of Binary Kloosterman Sum

When looking for zeros of binary Kloosterman sums, which is of high cryptographic interest as Table 2 emphasizes, one benefits from even more properties of elliptic curves over finite fields. Indeed, when $K_m(a) = 0$, we get that $\#E_m(a) = 2^m$. Hence all rational points of $E_m(a)$ are of order some power of 2.

In fact, we know even more. As $E_m(a)$ is defined over a field of characteristic 2, its complete 2^e-torsion (where e is any strictly positive integer) is of rank 1, whereas the complete l^e-torsion, for a prime l different from 2, is of rank 2, as stated in Proposition 6. Therefore the rational Sylow 2-subgroup is cyclic, isomorphic to $\mathbb{Z}/2^e\mathbb{Z}$ for some positive integer e. In the case $K_m(a) = 0$, we even get that the whole group of rational points is isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$. Furthermore, basic group theory tells that $E_m(a)$ will then have 2^{m-1} points of order 2^m.

Finally it should be noted that if $2^m \mid \#E_m(a)$, then $\#E_m(a)$ must be equal to 2^m. This is a simple consequence of Hasse theorem 5 giving bounds on the number of rational points of an elliptic curve over a finite field.

These facts have first been used by Lisoněk in [26] to develop a probabilistic method to test whether a given a is a binary Kloosterman zero or not: one takes a random point on $E_m(a)$ and tests whether its order is 2^m or not. This test involves at most m duplications on the curve, hence is quite efficient. Moreover, as soon as $\#E_m(a) = 2^m$, half of its points are generators, so that testing one point on a correct curve gives a probability of success of 1/2. This led Lisoněk to find zeros of binary Kloosterman sums for m up to 64 in a matter of days.

Afterwards Ahmadi and Granger proposed in [1] a deterministic algorithm to test whether an element $a \in \mathbb{F}_{2^m}$ is a binary Kloosterman zero or not. From the above discussion, it is indeed enough to compute the size of the Sylow 2-subgroup of $E_m(a)$ to answer that question. This can be efficiently implemented by point halving, starting from a point of order 4. The complexity of each iteration of their algorithm is dominated by two multiplications in $\mathbb{F}_{2^m}$. So testing a curve

with a Sylow 2-subgroup of size 2^e is of complexity $O(e \cdot m \log m \log\log m)$. Furthermore, they showed that the average size of the Sylow 2-subgroup of the curves of the form $E_m(a)$ is 2^3 when m goes to infinity, so that their algorithm has an average bit complexity of $O(m \log m \log\log m)$.

4.3 Implementation for the Value 4

As shown in Table 2, we have a necessary and sufficient condition to build bent functions from the value 4 of binary Kloosterman sums when m is odd and a necessary condition only when m is even. However the situation is more complicated than in the case of binary Kloosterman zeros.

We are looking for $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$. The cardinality of $E_m(a)$ should then be $\#E_m(a) = 2^m + K_m(a) = 4(2^{m-2} + 1)$ which does not ensure to have a completely fixed group structure as in the case where $\#E_m(a) = 2^m$. Moreover, in general, the number $2^{m-2} + 1$ does not verify many divisibility properties leading to an efficient test for the value 4. The cardinality of the twist $\widetilde{E}_m(a)$ is given by $\#\widetilde{E}_m(a) = 2^m + 2 - K_m(a) = 2(2^{m-1} - 1)$ which does not provide more useful information.

What we can however deduce from these equalities is that if $K_m(a) = 4$, then:

- $K_m(a) \equiv 4 \pmod 8$, so that $\mathrm{Tr}_1^m(a) = 1$;
- $K_m(a) \equiv 1 \pmod 3$, so that:
  - if m is odd, then a can be written as $t^4 + t^3$;
  - if m is even, then a can be written as t^3 with $\mathrm{Tr}_2^m(t) \neq 0$.

We can use both these conditions to filter out a to be tested as described in Algorithm 1 (for m odd).

Algorithm 1: Finding the value 4 of binary Kloosterman sums for m odd

Input: A positive odd integer $m \geq 3$
Output: An element $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$

```
1  a ←_R F_{2^m}
2  a ← a^3(a + 1)
3  if Tr_1^m(a) = 0 then
4  |  Go to step 1
5  P ←_R E_m(a)
6  if [2^m + 4]P ≠ 0 then
7  |  Go to step 1
8  if #E_m(a) ≠ 2^m + 4 then
9  |  Go to step 1
10 return a
```

We implemented this algorithm in Sage [36]. It was necessary to implement a relatively efficient version of point counting in characteristic 2, none of them being available. The exact algorithm chosen was an extension to characteristic 2 of Satoh's original algorithm by Fouquet, Gaudry and Harley [16]. The complexity of this algorithm is $O(m^{3+\epsilon})$ bit operations (or $O(m^5)$ with naïve multiplication) and $O(m^3)$ memory, but it is quite simple and there was already an existing implementation in GP/Pari by Yeoh [40] to use as a starting point. The computations in

$\mathbb{Z}_{2^m}$, the unique unramified extension of degree m of the 2-adic integers $\mathbb{Z}_2$, were done through the direct library interface to Pari [30] provided in Sage. Our implementation has been contributed back to Sage[1]. As a byproduct of our work we corrected and optimized the current implementation of Boolean functions in Sage[2]. The code for manipulating binary Kloosterman sums has also been made available on one author's homepage[3].

As a result of our experiments, we found that the following value of a for $m = 55$ gives a value 4 of binary Kloosterman sum. The finite field $\mathbb{F}_{2^{55}}$ is represented as $\mathbb{F}_2[x]/(x^{55} + x^{11} + x^{10} + x^9 + x^7 + x^4 + 1)$; a is then given as:

$$\begin{aligned} a = {} & x^{53} + x^{52} + x^{51} + x^{50} + x^{47} + x^{43} + x^{41} + x^{38} + x^{37} + x^{35} \\ & + x^{33} + x^{32} + x^{30} + x^{29} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} \\ & + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{15} + x^{13} + x^{12} + x^5 \ . \end{aligned}$$

5 Experimental Results for m Even

When m is even, Mesnager has showed in [28] that the situation seems to be more complicated theoretically than in the case where m is odd and that the study of the bentness of the Boolean functions given in Table 2 cannot be done as in the odd case. As shown in Table 2 we only have a necessary condition to build bent functions from the value 4 of binary Kloosterman sum when m is even. To get a better understanding of the situation we conducted some experimental tests to check whether the Boolean functions constructed with the formula of Table 2 were bent or not for all the a's in $\mathbb{F}_{2^m}$ giving a value 4.

Therefore we define for $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$ the Boolean function $f_{a,b}$ with $n = 2m$ inputs as:

$$f_{a,b}(x) = \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \ . \tag{1}$$

We now show that it is enough to test the bentness of a subset of these functions to get results about all of them.

First of all, the next proposition proves that the study of the bentness of $f_{a,b}$ can be reduced to the case where $b = 1$.

Proposition 16. *Let $n = 2m$ with $m \geq 3$ even. Let $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by Equation (1). Then $f_{a,b}$ is bent if and only if $f_{a,1}$ is bent.*

Proof. Since m is even, $\mathbb{F}_4^* \subset \mathbb{F}_{2^m}^*$. In particular, for every $b \in \mathbb{F}_4^*$, there exists $\alpha \in \mathbb{F}_{2^m}^*$ such that $\alpha^{\frac{2^n-1}{3}} = b$. For $x \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned} f_{a,b}(x) &= \mathrm{Tr}_1^n\left(ax^{2^m-1}\right) + \mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right) \\ &= \mathrm{Tr}_1^n\left(a\alpha^{2^m-1}x^{2^m-1}\right) + \mathrm{Tr}_1^2\left(\alpha^{\frac{2^n-1}{3}}x^{\frac{2^n-1}{3}}\right) \\ &= \mathrm{Tr}_1^n\left(a(\alpha x)^{2^m-1})\right) + \mathrm{Tr}_1^2\left((\alpha x)^{\frac{2^n-1}{3}}\right) \\ &= f_{a,1}(\alpha x) \ . \end{aligned}$$

[1] `http://trac.sagemath.org/sage_trac/ticket/11448`
[2] `http://trac.sagemath.org/sage_trac/ticket/11450`
[3] `http://perso.telecom-paristech.fr/~flori/kloo/`

Hence, for every $\omega \in \mathbb{F}_{2^n}^*$, we have

$$\begin{aligned}\widehat{\chi_{f_{a,b}}}(\omega) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{a,b}(x)+\mathrm{Tr}_1^n(\omega x)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{a,1}(\alpha x)+\mathrm{Tr}_1^n(\omega x)} \\ &= \widehat{\chi_{f_{a,1}}}(\omega\alpha^{-1}) \ .\end{aligned}$$

□

Second, we know that $K_m(a) = K_m(a^2)$, so the $a \in \mathbb{F}_{2^m}$ giving a value 4 of binary Kloosterman sums come in cyclotomic classes. Fortunately it is enough to check one a per class. Indeed $f_{a,b}$ is bent if and only if f_{a^2,b^2} is, as proved in the following proposition.

Proposition 17. *Let $n = 2m$ with $m \geq 3$. Let $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let $f_{a,b}$ be the function defined on $\mathbb{F}_{2^n}$ by Equation* (1)*. Then $f_{a,b}$ is bent if and only if f_{a^2,b^2} is bent.*

Proof.

$$\begin{aligned}\widehat{\chi_{f_{a,b}}}(\omega) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{a,b}(x)+\mathrm{Tr}_1^n(\omega x)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(ax^{2^m-1}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n(\omega x)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(a^2x^{2^{2m}-1}\right)+\mathrm{Tr}_1^2\left(b^2x^{2\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n\left(\omega^2x^2\right)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n\left(a^2x^{2^m-1}\right)+\mathrm{Tr}_1^2\left(b^2x^{\frac{2^n-1}{3}}\right)+\mathrm{Tr}_1^n\left(\omega^2x\right)} \\ &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f_{a^2,b^2}(x)+\mathrm{Tr}_1^n\left(\omega^2x\right)} \\ &= \widehat{\chi_{f_{a^2,b^2}}}(\omega^2) \ .\end{aligned}$$

□

In the specific case $b = 1$ that we are interested in, it gives that $f_{a,1}$ is bent if and only if $f_{a^2,1}$ is, which proves that checking one element of each cyclotomic class is enough.

Finally, as mentioned in Sect. 4, finding all the a's in $\mathbb{F}_{2^m}$ giving a specific value is a different problem from finding one such $a \in \mathbb{F}_{2^m}$. One can compute the Walsh-Hadamard transform of the trace of inverse using a fast Walsh-Hadamard transform. As long as the basis of $\mathbb{F}_{2^m}$ considered as a vector space over $\mathbb{F}_2$ is correctly chosen so that the trace corresponds to the scalar product, the implementation is straightforward.

The algorithm that we implemented is described in Algorithm 2. The implementation[3] was made using Sage [36] and Cython [4], performing direct calls to Givaro [14], NTL [34] and gf2x [5] libraries for efficient manipulation of finite field elements and construction of Boolean functions.

In Table 4 we give the results of the computations we conducted along with different pieces of information about them. One should remark that all the Boolean functions which could be tested are bent. Evidence that our computations were correct is given by the fact that the number of cyclotomic classes we found is so. This can be checked using the formula of

Algorithm 2: Testing bentness for m even

Input: An even integer $m \geq 3$

Output: A list of couples made of one representative for each cyclotomic class of elements $a \in \mathbb{F}_{2^m}$ such that $K_m(a) = 4$ together with 1 if the corresponding Boolean functions $f_{a,b}$ are bent, 0 otherwise

```
Build the Boolean function f : x ∈ F_{2^n} ↦ Tr_1^n(1/x) ∈ F_2
Compute the Walsh-Hadamard transform of f
Build a list A made of one a ∈ F_{2^m} for each cyclotomic class such that K_m(a) = 4
Initialize an empty list R
foreach a ∈ A do
    Build the Boolean function f_{a,1}
    Compute the Walsh-Hadamard transform of f_{a,1}
    if f_{a,1} is bent then
        Append (a, 1) to R
    else
        Append (a, 0) to R
return R
```

Table 4: Test of bentness for m even

m	Nb. of cyclotomic classes	Time	All bent?
4	1	<1s	yes
6	1	<1s	yes
8	2	<1s	yes
10	3	4s	yes
12	6	130s	yes
14	8	3000s	yes
16	14	82000s	yes
18	20	-	-
20	76	-	-
22	87	-	-
24	128	-	-
26	210	-	-
28	810	-	-
30	923	-	-
32	2646	-	-

Table 5: The fourteen cyclotomic classes such that $K_{16}(a) = 4$ as elements of $\mathbb{F}_2[x]/(x^{16} + x^5 + x^3 + x^2 + 1)$

$$
\begin{array}{l}
x^{14} + x^{11} + x^8 + x^6 + x^3 + x \\
x^{15} + x^{13} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1 \\
x^{14} + x^{13} + x^{12} + x^{10} + x^8 + x^2 + x \\
x^{14} + x^{12} + x^{11} + x^9 + x^6 + x \\
x^{15} + x^{11} + x^9 + x^7 + x^6 + x^3 + x^2 + 1 \\
x^{13} + x^6 + x^4 + x^2 + x + 1 \\
x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^3 + x^2 + x \\
x^{15} + x^{11} + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 \\
x^{15} + x^{13} + x^9 + x^8 + x^5 + x^4 + x^3 + x \\
x^{15} + x^{11} + x^{10} + x^3 \\
x^{13} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^3 + x^2 + x \\
x^{13} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x \\
x^{15} + x^{13} + x^{10} + x^9 + x^8 + x^7 + x^5 + x \\
x^{15} + x^{11} + x^{10} + x^3 + x + 1
\end{array}
$$

Proposition 8. We are looking for elliptic curves with trace t of the Frobenius automorphism equal to $t = 1 - K_m(a) = -3$. Hence the number of cycloctomic classes is $H(\Delta)/m$ where $\Delta = 9 - 4 \cdot 2^m$. Moreover, for the values we tested, except $m = 12, 30, 32$, this discriminant is fundamental, so that the order $\mathbb{Z}[\alpha]$ is maximal and $H(\Delta) = h(\Delta)$ the classical class number, a quantity even easier to compute.

Unfortunately we were not able to check bentness of functions for $m > 16$ due to lack of memory. Constructing the Boolean functions of $n = 2m$ variables is the most time consuming part of the test, but the real bottleneck is the amount of memory needed to compute their Walsh-Hadamard transform. One must indeed perform the Walsh-Hadamard transform using integers of size at least $2m + 1$ bits, so, with our implementation, integers of 64 bits from $m = 16$. The amount of memory needed is then $64 \cdot 2^{2m} \cdot 2^{-30} = 2^{2m-24}$ gigabytes. For $m = 16$ this represents already 32 GB of memory; for $m = 18$ it would be 512 GB of memory. Therefore we give in Table 5 the fourteen values of a found for $m = 16$, the highest value that we could test. The corresponding Boolean functions of $n = 32$ variables are all bent as we already pointed out. In Table 5, the finite field $\mathbb{F}_{2^{16}}$ is represented as $\mathbb{F}_2[x]/(x^{16} + x^5 + x^3 + x^2 + 1)$.

6 Conclusion

In this work we studied the different existing algorithms to compute or test zeros of binary Kloosterman sums in order to extend them to the computation of the value 4. This is a non-trivial problem because the situation for zeros of binary Kloosterman sums is very specific. Indeed, it involves results about the 2-torsion of elliptic curves over a finite field of characteristic 2 which can no longer be used when looking for the value 4. Nonetheless we showed that the theory of elliptic curves gives other necessary conditions that we used to implement an algorithm to find the value 4.

The case where m is odd is currently the most interesting from a cryptographic point of view because such values lead to the construction of hyperbent functions of $n = 2m$ variables. All of our code has been contributed to the Sage project or made available online.

When m is even, the situation is theoretically more complicated. It has been shown that the

value 4 is still a necessary condition, but it is an open problem to tell whether this condition is sufficient for all m even or not. Therefore we conducted experiments to find all the values 4 of binary Kloosterman sums and test the corresponding Boolean functions for m even as big as possible. All the values we tested gave bent functions, pointing out that the situation in the case m even should definitely be studied further.

References

[1] Omran Ahmadi and Robert Granger. An efficient deterministic test for Kloosterman sum zeros. *CoRR*, abs/1104.3882, 2011.

[2] J. Arndt. *Matters Computational: Ideas, Algorithms, Source Code*. Springer, 2010.

[3] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[4] R. Bradshaw, C. Citro, and D.S. Seljebotn. Cython: the best of both worlds. *CiSE 2011 Special Python Issue*, page 25, 2010.

[5] Richard P. Brent, Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann. Faster multiplication in GF(2)[x]. In Alfred J. van der Poorten and Andreas Stein, editors, *ANTS*, volume 5011 of *Lecture Notes in Computer Science*, pages 153–166. Springer, 2008.

[6] Claude Carlet. Boolean functions for cryptography and error correcting codes. In Yves Crama and Peter L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 257–397. Cambridge University Press, June 2010.

[7] Pascale Charpin and Guang Gong. Hyperbent functions, Kloosterman sums, and Dickson polynomials. *IEEE Transactions on Information Theory*, 54(9):4230–4238, 2008.

[8] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. Divisibility properties of classical binary Kloosterman sums. *Discrete Mathematics*, 309(12):3975–3984, 2009.

[9] Seongtaek Chee, Sangjin Lee, and Kwangjo Kim. Semi-bent functions. In Josef Pieprzyk and Reihaneh Safavi-Naini, editors, *ASIACRYPT*, volume 917 of *Lecture Notes in Computer Science*, pages 107–118. Springer, 1994.

[10] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[11] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[12] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[13] John Francis Dillon. *Elementary Hadamard Difference Sets*. ProQuest LLC, Ann Arbor, MI, 1974. Thesis (Ph.D.)–University of Maryland, College Park.

[14] Jean-Guillaume Dumas, Thierry Gautier, Pascal Giorgi, Jean-Louis Roch, and Gilles Villard. *Givaro-3.2.13rc1: C++ library for arithmetic and algebraic computations*, September 2008. `http://ljk.imag.fr/CASYS/LOGICIELS/givaro/`.

[15] Andreas Enge. *Elliptic Curves and Their Applications to Cryptography: An Introduction*. Springer, 1st edition, August 1999.

[16] Mireille Fouquet, Pierrick Gaudry, and Robert Harley. An extension of Satoh's algorithm and its implementation. *Journal of the Ramanujan Mathematical Society*, 15:281–318, 2000.

[17] Robert Harley. Asymptotically optimal p-adic point-counting. Email to NMBRTHRY list, December 2002. `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=nmbrthry&T=0&P=1343`.

[18] Tor Helleseth and Victor Zinoviev. On linear Goethals codes and Kloosterman sums. *Des. Codes Cryptography*, 17(1-3):269–288, 1999.

[19] Nicholas Katz and Ron Livné. Sommes de Kloosterman et courbes elliptiques universelles en caractéristiques 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 309(11):723–726, 1989.

[20] Neal Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 156–167. Springer, 1990.

[21] Gilles Lachaud and Jacques Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 305(20):881–883, 1987.

[22] Gilles Lachaud and Jacques Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Transactions on Information Theory*, 36(3):686Ð692, 1990.

[23] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[24] N. G. Leander. Monomial bent functions. *IEEE Transactions on Information Theory*, 52(2):738–743, 2006.

[25] Reynald Lercier, David Lubicz, and Frederik Vercauteren. Point counting on elliptic and hyperelliptic curves. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 407–453. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[26] Petr Lisonek. On the connection between Kloosterman sums and elliptic curves. In Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 182–187. Springer, 2008.

[27] Sihem Mesnager. A new family of hyper-bent Boolean functions in polynomial form. In Matthew G. Parker, editor, *IMA Int. Conf.*, volume 5921 of *Lecture Notes in Computer Science*, pages 402–417. Springer, 2009.

[28] Sihem Mesnager. A new class of bent and hyper-bent Boolean functions in polynomial forms. *Des. Codes Cryptography*, 59(1-3):265–279, 2011.

[29] Sihem Mesnager. Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. *IEEE Transactions on Information Theory*, To appear.

[30] The PARI Group, Bordeaux. *PARI/GP, version* `2.4.3`, October 2010. available from `http://pari.math.u-bordeaux.fr/`.

[31] O. S. Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976.

[32] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[33] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Comb. Theory, Ser. A*, 46(2):183–211, 1987.

[34] Victor Shoup. NTL 5.4.2: A library for doing number theory, March 2008. `www.shoup.net/ntl`.

[35] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[36] W. A. Stein et al. *Sage Mathematics Software (Version 4.7)*. The Sage Development Team, 2011. `http://www.sagemath.org`.

[37] F. Vercauteren. Advances in point counting. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 103–132. Cambridge Univ. Press, Cambridge, 2005.

[38] Frederik Vercauteren. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2003.

[39] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[40] Yeoh. GP/Pari implementation of point counting in characteristic 2. `http://pages.cs.wisc.edu/~yeoh/nt/satoh-fgh.gp`.

[41] Nam Yul Yu and Guang Gong. Constructions of quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, 52(7):3291–3299, 2006.